AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1) Samsung Galaxy S10 plus, IMEI 35Z689100035584
2) Nokia Phone Model 6102i, IMEI 359373/00/434485/7
CURRENTLY IN THE CUSTODY OF FBI CINCINNATI

Case No. 1:20-mj-475

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1029	Access Device Fraud
18 U.S.C. 1343	Wire Fraud

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Devin Peugh, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.
(via FaceTime)

Date: 7/1/2020

Judge's signature

City and state: Cincinnati, Ohio

Hon. Karen L. Litkovitz, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is:

1) **Samsung Galaxy S10 plus, IMEI 35Z689100035584**
2) **Nokia Phone Model 6102i, IMEI 359373/00/434485/7**

The devices are currently in the custody of FBI Cincinnati.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 USC 1029 and 18 USC 1343, including:

   a. The evidence, fruits and instrumentalities of access device fraud, including:

      i. Any access device, account credentials, or means of identification of another;

      ii. Any access device manufacturing implements or materials, to include encoders, embossers and cards, and other devices and/or equipment to manufacturer cards;

      iii. Any software to facilitate access device fraud;

      iv. Any record of connection to a device that facilitates access device fraud;

      v. Any receipt or document in any form showing the use of access devices, account credentials, or other means to fraudulently purchase goods or services;

      vi. Any receipt, document or card in any form used for the purpose of or documenting the transfer of funds;

      vii. Any packaging or correspondence used to transfer items between parties;

      viii. Any geo-location information; and

      ix. Any stored communication in any form between pertaining to the use of unauthorized access devices, account credentials, or other supporting activities.

   b. Records and information relating to a conspiracy to defraud any victims;

   c. Usernames, passwords, PIN numbers, and other account credentials or account identifiers of any victims;

   d. Records and information relating to access to sites on the "dark web";

   e. Records and information relating to any assets, bank accounts, money transfer transactions, or Bitcoin accounts;

   f. Records and information relating to the purchase, sale, re-encoding, or trafficking of bank account or credit account numbers or other means of identifications;

g. Records and information relating to the identity, location, or travel, of individuals involved in fraudulent activities;

h. Records or information relating to the assets or finances of individuals involved in fraudulent activities;

i. Records and information of utilization of email accounts, social media accounts, and online chat programs.

j. Records and information relating to utilization of aliases and fictitious names.

k. Records of address or identifying information for individuals using the electronic evidence, and any personal or business contacts or associates of his, (however and wherever written, stored, or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user IDs, eIDs (electronic ID numbers), and passwords; and

l. Any photograph, calendar entry, or other item in any format that directly or indirectly relates to the use of unauthorized access device or other supporting activities.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF: 1) **Samsung Galaxy S10 plus, IMEI 35Z689100035584** 2) **Nokia Phone Model 6102i, IMEI 359373/00/434485/7** CURRENTLY IN THE CUSTODY OF FBI CINCINNATI	Case No. 1:20-mj-475

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Devin Peugh, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the Federal Bureau of Investigation since March 2019, and am currently assigned to the Cincinnati Division. Prior to my employment as a Special Agent, I was employed for five years as a Staff Operations Specialist for the Federal Bureau of Investigation, assigned to the San Diego Division. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology or cybercrime, child pornography, terrorism, money laundering, and credit card fraud. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of an application for a search warrant for the electronic devices described in Attachment A ("TARGET DEVICES"), which are currently in law enforcement possession, and the extraction from the TARGET DEVICES of electronically stored information described in Attachment B.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PERTINENT FEDERAL CRIMINAL STATUTES

4. 18 U.S.C. § 1029(b)(2) – Conspiracy to Commit Access Device Fraud

5. 18 U.S.C. § 1349 – Conspiracy to Commit Bank Fraud

Background on Credit Card Skimmers

6. The FBI has been investigating a credit card fraud scheme which utilizes skimming devices ("skimmers") placed on and inside ATMs in the Southern District of Ohio, which acquire credit and debit card information from victims.

7. Based on my training and experience, I know that it is possible to re-encode digitally stored account information onto the magnetic strip of any type of plastic access device using commercially available digital reader-writer devices and the corresponding computer software that comes with the devices. These devices and this software have legitimate commercial uses such as coding hotel room keys and creating security badges.

8. Based on my training and experience, I know that subjects that use fraudulently re-encoded credit and debit cards purchase prepaid credit cards as a way to conceal the illegitimate source of funds and carry on the fraud. Prepaid credit and debit cards are also a common tool for perpetrators of fraud and identity theft. The perpetrators can also use the

prepaid cards to re-encode compromised credit card account data onto access devices which they then use to make fraudulent purchases such as additional prepaid credit cards at stores such as Walmart and Kroger.

9. The process of purchasing prepaid credit cards at retail stores involves the transmission of electronic communications via wire communication between the point of sale and the bank that holds the compromised account that is being charged for the transaction, and the bank that issued the prepaid credit card. These communications are transmitted in interstate commerce because the various banks are located in different states from each other and from the points of sale, and because communications sent via wire communications travel interstate based on the locations of the service providers.

10. Through my training and experience, I know skimmers to be devices used to covertly collect credit and/or debit card data from victims. The illegally collected credit and debit card numbers are considered access devices. The credit and debit card number related to a victim's account and the cards and card numbers are issued by banks which are federally insured financial institutions.

11. A "skimmer" placed inside an ATM collects card information from victims when that victim uses a card at the ATM. The skimmer is installed between the credit card reader and the other internal circuitry of the ATM. In addition to the skimmer, the subjects may also install a camera on the face of the ATM to capture entries made by customers on the pin pad of the ATM. This is used to obtain both the card number and corresponding PIN for the card.

12. The skimmer usually does not keep the ATM from otherwise functioning properly; the intended transaction will typically proceed without interruption of any kind or any

notification to the victim or third party. Because of this and the fact that the skimmer is installed inside the ATM, it is impossible for victims using the ATM to detect the presence of the skimmer. Additionally, the skimmer does not require a successful transaction to collect the card data; the card data is collected when the victim swipes their card.

13. A single skimmer is capable of storing card information for hundreds of victims. A credit or debit card contains a magnetic strip that contains information such as the card holder's name, card number, and expiration date. The victim card data is then used to create a clone of the compromised credit card by re-encoding another card, such as a prepaid card or gift card, with victim card information.

14. To make the card appear more legitimate to third parties, the subjects may use a credit card embossing device to physically stamp a name of their choosing onto the newly written card.

15. Based on my training and experience I know that individuals involved in ATM skimming activity typically use re-encoded cards at ATMs to withdraw cash from the associated account. The subjects use a variety of equipment to re-encode cards such as card reader/writers, laptops or computers with software specifically designed to read/write data to cards.

16. Based on my training and experience I know that individuals sometimes work in groups in furtherance of skimming activity. Once an individual manufactures a skimmer, that individual will use the skimmer in one or more of the following ways: First, the individual can personally use the skimmer to collect card information. Second, the individual can sell the device to another person who will then use the device to collect card information. Third, the individual can provide the device to another person in return for a portion of cards collected by

the device as payment. The re-encoded cards can then be used to purchase prepaid goods and services, cashed out, or sold to other individuals.

17. Based on my training and experience I know that individuals involved in skimming sometimes travel from one region to another inserting skimmers, re-encoding cards, and conducting cash out ATM transactions. This sometimes requires individuals involved in skimming to travel with the requisite electronics to conduct skimming activities.

PROBABLE CAUSE

18. On September 4, 2019, the Colerain Police Department alerted the FBI that a financial institution (hereafter Financial Institution-1) located in Colerain Township, Ohio, and headquartered in the Southern District of Ohio, had detected ATM skimming activity at one of Financial Institution-1's ATMs (hereafter ATM-1). On September 5, 2019, Financial Institution-1 provided ATM camera footage to the FBI. A review of this camera footage revealed the following:

a. On August 7, 2019, at approximately 6:53am, an individual with a gray sweatshirt, gray t-shirt, dark baseball hat, with a dark beard and mustache (hereafter Individual-1) approached ATM-1 on foot. Individual-1 proceeded to remove a long dark bar from his sweatshirt and place it below the face of ATM-1. Based on my training and experience, I know that when installing a skimming device individuals will typically also install a camera facing the pin pad of the ATM in order to capture the PIN numbers entered by customers. At approximately 6:54am, Individual-1 departed from ATM-1 on foot.

b. On August 7, 2019, at approximately 7:00am, an individual wearing a black t-

shirt and gray baseball hat, with dark facial hair, later identified as GEORGIAN GOREA (GOREA), approached ATM-1 on foot carrying what appeared to be an electronic device. GOREA proceeded to insert the device into ATM-1's card reader. GOREA then removed a card from his wallet and inserted the card into ATM-1's card reader. GOREA inserted the card into ATM-1's card reader multiple times while manipulating the face of ATM-1. During this process GOREA did not receive any cash or receipts from ATM-1. Based on my training and experience, I believe GOREA installed a skimmer inside of ATM-1 and was inserting cards to ensure it had been installed properly. At approximately 7:00am, GOREA departed from ATM-1 on foot.

c. On August 11, 2019, at approximately 8:58pm, Individual-1 approached ATM-1 on a bicycle. Individual-1 then removed a contraption from the basket of the bicycle. Individual-1 proceeded to use this contraption to remove a device from ATM-1. Individual-1 continued to manipulate the face of ATM-1 and removed the black bar installed beneath the face of ATM-1. At approximately 8:59pm, Individual-1 departed on a bicycle from ATM-1.

19. Financial Institution-1 provided the FBI a list of approximately 342 debit card numbers that had been compromised as a result of the skimming device installed on ATM-1 from August 7, 2019, to August 11, 2019. This list included the locations of any cash out attempts conducted using the compromised card numbers. The majority of these cash out attempts occurred at ATMs at another Financial Institution (hereafter Financial Institution-2).

20. Based on my training and experience I know individuals involved in card

skimming will encode compromised card numbers onto blank magnetic stripe cards which are then used to conduct ATM cash withdrawals from the compromised card account.

21. Financial Institution-2 provided the FBI with ATM camera photos of Individual-1, GOREA, an individual later identified as VALERICA IVANOVICI (IVANOVICI), and an individual later identified as ZLATKO MARIUS GALEATOVICI (GALEATOVICI), using the compromised card numbers taken from Financial Institution-1 to conduct cash withdrawals at approximately 16 of Financial Institution-2's ATMs. These 16 ATMs were located in the Southern District of Ohio. A review of Financial Institution-2's ATM camera photos combined with a review of the compromised card numbers provided by Financial Institution-1, revealed Individual-1, GOREA, IVANOVICI, and GALEATOVICI were using the compromised card numbers obtained from the skimming device previously installed on ATM-1 to conduct their cash out transactions between August 31, 2019 and September 3, 2019.

22. On October 16, 2019, Financial Institution-1 contacted the FBI and reported that a skimming device had been installed on Financial Institution-1's ATM located in Celina, Ohio (hereafter ATM-4).

23. Financial Institution-1 provided the FBI with ATM-4's camera footage which captured the installation and removal of a skimming device on ATM-4. A review of this footage revealed the following information:

a. On September 28, 2019, at approximately 7:15am, ATM-4's camera captured GOREA arriving at ATM-4 in a dark color Toyota sport utility vehicle. GOREA then exited the vehicle and, after multiple attempts, successfully installed an electronic device into ATM-4's card reader. GOREA then inserted a magnetic

stripe card into ATM-4's card reader. While GOREA conducted this activity, ATM-4's camera captured GALEATOVICI sitting in the rear driver's side seat of the vehicle. GOREA then returned to the vehicle and maneuvered the vehicle closer to ATM-4. After re-positioning the vehicle, ATM-4's camera captured GOREA manipulating and compromising the face of ATM-4. GOREA then installed a black bar beneath the face of ATM-4.

b. On September 29, 2019, at approximately 8:56am, ATM-4's camera captured GOREA approaching ATM-4 in a dark color Toyota sport utility vehicle. GOREA proceeded to remove a black bar from beneath the face of ATM-4. At approximately 8:57am, GOREA departed from ATM-4.

c. On September 29, 2019, at approximately 11:03am, ATM-4's camera captured GALEATOVICI approaching ATM-4 on foot. GALEATOVICI attempted to conceal his face from ATM-4's camera while approaching ATM-4. GALEATOVICI arrived at ATM-4, covered ATM-4's camera and appeared to insert an object into ATM-4's card reader and manipulate the face of ATM-4. GALEATOVICI departed ATM-4 on foot at approximately 11:03am.

24. Through discussions with federal law enforcement partners I learned that another federal law enforcement agency conducted a search of a vacation rental rented by IVANOVICI using the alias Zoltan Toth. This search identified materials that law enforcement officers believed were used to build skimming devices in IVANOVICI's rented residence.

25. Vacation rental companies HomeAway and Airbnb provided the FBI with records regarding IVANOVICI's vacation rental history. I have reviewed this rental history and based on

this review have learned that IVANOVICI's rental reservations and reservation inquiries identified IVANOVICI as the sole occupant of the vacation rental.

26. In December 2019, another FBI Agent and I interviewed the owner of a vacation rental in Cincinnati, Ohio, where IVANOVICI stayed in early 2019. The owner of the residence was shown a photograph of IVANOVICI and immediately identified IVANOVICI as "Zoltan Toth." The owner indicated IVANOVICI stayed at the Cincinnati, Ohio vacation rental for a period of two months, during which time IVANOVICI was the sole occupant of the rental. IVANOVICI had no guests at the vacation rental during this two month span.

27. Based on my training and experience, I know that individuals involved in ATM skimming activities typically conduct these activities as part of a group. The members of these groups will often travel from city to city together for the purpose of conducting ATM skimming activities. Given the transient nature of this activity, ATM skimmers often use mobile communications to coordinate which cities, and more specifically ATMs, to visit at specific dates and times.

28. Through discussions with other law enforcement partners I was able to identify GOREA through a comparison of ATM photographs of GOREA with a photograph used by GOREA on a prior visa application.

29. Through discussions with other law enforcement partners I learned that IVANOVICI's identity was determined through a comparison of ATM photos with a photograph used by IVANOVICI on a prior visa application.

30. On December 29, 2019, the Evansville Police Department in Indiana arrested GALEATOVICI at an ATM while conducting cash withdrawals using card numbers

compromised from a financial institution in Indiana. At the time of his arrest GALEATOVICI provided identity documents bearing the name David L. Lakatos. GALEATOVICI's fingerprints were used to identify GALEATOVICI from a prior visa application.

31. On May 24, 2020, IVANOVICI flew to the George Bush Intercontinental Houston Airport ("IAH") aboard United Airlines flight 1091. Upon IVANOVICI's arrival in the United States FBI Agents assigned to IAH arrested IVANOVICI pursuant to an arrest warrant issued in the Southern District of Ohio where IVANOVICI was charged with 18 U.S.C. § 1029(b)(2) and 18 U.S.C. § 1349. At the time of his arrest IVANOVICI had one gray roller suitcase in his possession. FBI Houston sent this suitcase to FBI Cincinnati to be held until IVANOVICI's property could be returned. Upon receipt of IVANOVICI's gray roller suitcase, FBI Cincinnati conducted an inventory search of the suitcase's contents which revealed two cell phones; one **Samsung Galaxy S10 plus, IMEI 35Z689100035584** and one **Nokia Phone Model 6102i, IMEI 359373/00/434485/7 ("TARGET DEVICES")**. The TARGET DEVICES are currently held in the FBI Cincinnati Field Office.

32. Based on my training and experience, I know that individuals who are involved in a fraud scheme occurring in multiple cities and states often communicate with each other using devices such as cell phones to coordinate travel plans and location information. I also know that individuals who frequently communicate with each other save name and telephone number information in the phone's contact list. Therefore, it is reasonable to believe that co-conspirator contact information and their respective travel information would be contained on the TARGET DEVICES, and the extraction of such evidence would aid the government in locating GOREA and other unidentified subjects.

33. Based on the aforementioned, there is probable cause to believe that there is evidence of bank fraud and access device fraud on the TARGET DEVICES, as well as information regarding the true identity of Individual-1 and information that will assist in locating Individual-1, GOREA, and other co-conspirators.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

34. As described above and in Attachment B, this application seeks permission to search for records that might be found in the TARGET DEVICES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

35. *Probable cause.* There is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

36. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium or phone because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely

accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to engage in fraudulent activities, the individual's computer will generally serve both as an instrumentality for

committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

37. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic

evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

39. I submit that this affidavit supports probable cause for a warrant to search the TARGET DEVICES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

40. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Devin Peugh
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on July 1, 2020

THE HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is:

1) Samsung Galaxy S10 plus, IMEI 35Z689100035584
2) Nokia Phone Model 6102i, IMEI 359373/00/434485/7

The devices are currently in the custody of FBI Cincinnati.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 USC 1029 and 18 USC 1343, including:

   a. The evidence, fruits and instrumentalities of access device fraud, including:

      i. Any access device, account credentials, or means of identification of another;

      ii. Any access device manufacturing implements or materials, to include encoders, embossers and cards, and other devices and/or equipment to manufacturer cards;

      iii. Any software to facilitate access device fraud;

      iv. Any record of connection to a device that facilitates access device fraud;

      v. Any receipt or document in any form showing the use of access devices, account credentials, or other means to fraudulently purchase goods or services;

      vi. Any receipt, document or card in any form used for the purpose of or documenting the transfer of funds;

      vii. Any packaging or correspondence used to transfer items between parties;

      viii. Any geo-location information; and

      ix. Any stored communication in any form between pertaining to the use of unauthorized access devices, account credentials, or other supporting activities.

   b. Records and information relating to a conspiracy to defraud any victims;

   c. Usernames, passwords, PIN numbers, and other account credentials or account identifiers of any victims;

   d. Records and information relating to access to sites on the "dark web";

   e. Records and information relating to any assets, bank accounts, money transfer transactions, or Bitcoin accounts;

   f. Records and information relating to the purchase, sale, re-encoding, or trafficking of bank account or credit account numbers or other means of identifications;

g. Records and information relating to the identity, location, or travel, of individuals involved in fraudulent activities;

h. Records or information relating to the assets or finances of individuals involved in fraudulent activities;

i. Records and information of utilization of email accounts, social media accounts, and online chat programs.

j. Records and information relating to utilization of aliases and fictitious names.

k. Records of address or identifying information for individuals using the electronic evidence, and any personal or business contacts or associates of his, (however and wherever written, stored, or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user IDs, eIDs (electronic ID numbers), and passwords; and

l. Any photograph, calendar entry, or other item in any format that directly or indirectly relates to the use of unauthorized access device or other supporting activities.